Published and Copyright (c) 1999 - 2008
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1141 10/09/09

~ FBI Busts Phishing Ring ~ People Are Talking! ~ New Sony Laptop!
~ Hackers Expose Hotmail ~ Comcast Tries Alerts! ~ Win 8, 128-bit?
~ WW III in Cyberspace? ~ No Facebook at Work! ~ Password Primer!

~ ~ EA’s Dante’s Inferno! ~

-* Phishing Attacks Are Growing *-
-* EU To Finally Settle with Microsoft? *-
-* Net Neutrality Bill Faces GOP Opposition! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

Well, it’s a bachelor’s weekend around here; or, I should say, a long 10-day holiday weekend of sorts! It will just be me and the canine kids while my wife is off on a cruise with her mother up the northeast Canadian coast. So, we’ll see how this goes!

Interesting articles in this week’s issue. Too bad we’ll be missing Joe’s column this week, because I’d be interested in reading what Joe thinks of President Obama’s winning of the Nobel Peace Prize. I have to say that my first reaction when I heard the news was: "For what??" I still have to say my feeling hasn’t changed. Anyway, Joe’s words of wisdom will have to wait a week while he recuperates from some testing and subsequent medical treatment.

Another news tidbit that I saw, and included in this week’s issue, is a story about many companies not allowing employees to use social network sites like Facebook while at work. D’uh! Like that’s a decision that is ground-breaking policy! Hmmm, you’re at work, doing your job - should you be on the internet, playing around on Facebook? Or any other social networking site? Or, on the internet for non-work surfing? Hello??!!

Okay, let’s get right to this week’s issue, and I’ll get ready for the long holiday weekend, and some extra days of "bachelorhood"!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Dante’s Inferno Taking Players to Hell!
""""""""""""""""""""""""""""""""

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!

"""""""""""""""""""""""""""""""""""""

Dante’s Inferno Videogame Taking Players to Hell

US videogame titan Electronic Arts (EA) said Friday that an acclaimed Hollywood screenwriter has tackled the story line for a videogame taking players into Dante’s Inferno.

Visceral Games, the EA studio behind the "Dead Space" franchise, is having Will Rokos craft a videogame story from the first part of Dante Alighieri’s epic poem The Divine Comedy.

"Taking such a naturally rich and deep universe and adapting for the video game has been one of the most interesting and challenging projects I’ve worked on," said Rokos, who co-wrote the 2001 film ’Monster’s Ball.’

"I really got into re-imagining Dante as a flawed hero with a dark past, and his determination to save the love of his life from a terrible fate. It was a truly unique experience to re-create one man’s hell, one circle at a time."

The three-part poem written by the Italian author in the early 1300s tells of a journey through hell, purgatory, and heaven. Inferno is the first part.

"The task of adapting a revered and classic piece of literature for the gaming medium was a tremendous challenge," said Jonathan Knight, executive producer of ’Dante’s Inferno’ videogame.

"Dante Alighieri’s masterpiece forms the foundation of the game’s plot, but Will’s take on the Dante/Beatrice story brought the necessary conflict and action that made the material really work dramatically."

Players will assume the role of Dante as he fights through Alighieri’s nine circles of hell - limbo, lust, gluttony, greed, anger, heresy, violence, fraud and treachery.

"Inferno" will be released in Europe and North America in February of next year, according to EA.

Game software will be tailored for play on Microsoft Xbox 360 and Sony PlayStation 3 consoles along with PlayStation PSP handheld devices.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

EU Prepares To Settle Microsoft Browser Case

Microsoft Corp., which has already shelled out $2.5 billion in antitrust fines in Europe, is on the brink of closing a chapter in its long-running battle with regulators there, just in time for another to begin.

European regulators said Wednesday they were preparing to settle their investigation into the way Microsoft includes its market-leading Internet Explorer Web browser with the Windows operating system. Competing software makers had complained PC users didn't have a clear way to choose a browser that challenges Internet Explorer, and the European Commission concluded in January that Microsoft was violating antitrust laws.

Now, the regulators in Brussels say they will move forward with a proposal made by Microsoft in July that aims to give Windows users in Europe a better tool for choosing different Web browsers.

At a news conference at Microsoft's headquarters Wednesday, the company's general counsel, Brad Smith, said the EU announcement was a big step toward ending the company's antitrust conflicts in Europe.

It also will free Microsoft's legal team to push the software maker's search deal with Yahoo Inc. over regulatory hurdles. In July, Yahoo agreed to let Microsoft handle its Web searches as part of a 10-year deal. Regulators in the U.S. and Europe will be looking into whether the deal will inhibit competition in the market for online advertising.

The EU-Microsoft agreement came about after meetings between Smith, who led the negotiations, his team of lawyers, and top European Commission regulators. Microsoft and the regulators also held about 20 videoconferences between Redmond and Brussels in the last few months, Smith said.

Microsoft first tried to satisfy regulators' concerns about the browser by offering to sell the forthcoming Windows 7 with no browser at all, but the EU rejected the plan, saying it offered less choice for PC users, not more.

Microsoft came back with a second proposal: to show EU users a prominent screen from which they could choose from a list of several browsers. The proposal was modified during talks between the software maker and regulators, and now includes a screen explaining what Web browsers are. PC users can click a "tell me more" button for details.

Users of Windows XP, Vista and Windows 7, which is due to launch Oct. 22, can then pick several browsers - listed in alphabetical order - to install along with or instead of Internet Explorer. They can come back to that screen later to change their browser choice.

Most people get their browsers pre-installed by a computer maker such as Dell Inc. or Hewlett-Packard Co., which under the proposal would be free to pick non-Microsoft browsers and disable IE. Even if a computer comes with Internet Explorer on it, however, users are free to download rivals such as Firefox, Apple's Safari or Google Chrome off the Internet.

Web browsers are free, so they don't directly make money for Microsoft or any other software maker. But Web browsers are important for branding, and for giving companies a way to better control their users' experience on the Internet. For example, Google released the Chrome

browser so it could ensure a smoother performance of online software applications it offers.

Regulators said the proposal must clear several more steps before PC users will see the browser-selection option in action, but that won't hold up the release of Windows 7 in Europe. The European Commission said it will now formally request feedback from computer manufacturers, software companies and consumers. They have a month to respond.

If all goes well, Microsoft said the browser-choice screens would be pushed out to PC users across the EU. The new software in most cases will be installed through the automatic tool that distributes security fixes and other updates.

"Microsoft's commitments would indeed address our competition concerns," Kroes said Friday. The proposal "would empower all current and future users of Windows in Europe to choose which browser they wished to use."

Microsoft also committed to share more information with software developers for the next 10 years to help them make products compatible with Windows and key pieces of software used in businesses: Windows Server, Office, Exchange and SharePoint. Microsoft agreed to make sure its technology is built using industry standards, after years of complaints from rivals about its proprietary choices for Web browsers and document formats.

Thomas Vinje, legal counsel for a group of companies that complained about Microsoft's business methods, said the settlement does not seem to deal with the flawed way that Microsoft applies standards, its unfair pricing practices or other concerns about patent abuse or standards manipulation.

Net Neutrality Rules Face Mounting GOP Opposition

Republican opposition is mounting as federal regulators prepare to vote this month on so-called "network neutrality" rules, which would prohibit broadband providers from favoring or discriminating against certain types of Internet traffic flowing over their lines.

Twenty House Republicans - including most of the Republicans on the House Energy and Commerce Committee - sent a letter to Federal Communications Commission Chairman Julius Genachowski on Monday urging him to delay the Oct. 22 vote on his net neutrality plan.

Genachowski, one of three Democrats on the five-member commission, wants to impose rules to ensure that broadband providers don't abuse their power over Internet access to favor their own services or harm competitors.

Democrats say the rules will keep phone companies from discriminating against Internet calling services and stop cable TV providers from hindering online video applications.

But in a letter to Genachowski on Monday, Rep. Cliff Stearns of Florida, the top Republican on the Subcommittee on Communications, Technology and the Internet, and his colleagues warned that new net neutrality regulations could discourage broadband providers from investing in their

networks. The letter said that if Internet service providers can’t manage traffic on their networks to ensure efficient service, consumers could suffer.

The Republicans are calling on Genachowski to conduct a "thorough market analysis" to determine whether new regulations are necessary.

Their points echoed those made in a letter that House Minority Leader John Boehner of Ohio and House Republican Whip Eric Cantor of Virginia sent to President Barack Obama on Friday.

Genachowski’s office had no comment on the letters.

Meanwhile in the Senate, the top Republican on the Commerce Committee, Kay Bailey Hutchinson of Texas, is considering legislation that would prohibit the FCC from developing net neutrality rules.

Genachowski’s proposal calls for the FCC to formally adopt four existing principles that have guided the agency’s enforcement of communications laws since 2005. Those principles state that network operators must allow subscribers to access all legal online content, applications, services and devices.

Genachowski is also calling for the FCC to adopt two additional principles that would prevent broadband providers from discriminating against particular content or applications and would require them to be open about their network management practices. And he is calling for the agency to apply these rules across different types of broadband networks, including wireless networks.

Hackers Expose Slew of Hotmail Acount Passwords

Microsoft blocked access to thousands of Hotmail accounts in response to hackers plundering password information and posting it online.

Cyber-crooks evidently used "phishing" tactics to dupe users of Microsoft’s free Web-based email service into revealing account and access information, according to the US technology giant.

"We are aware that some Windows Live Hotmail customers’ credentials were acquired illegally by a phishing scheme and exposed on a website," Microsoft said in response to an AFP inquiry.

"We have taken measures to block access to all of the accounts that were exposed and have resources in place to help those users reclaim their accounts."

Microsoft said it learned of the problem during the weekend after Hotmail account information of "several thousand" users, many of them reportedly in Europe, was posted at a website.

Phishing is an Internet bane and involves using what hackers refer to as "social engineering" to trick people into revealing information online or downloading malicious software onto computers.

Phishing tactics include sending people tainted email attachments that promise enticing content such as sexy photos of celebrities and luring

people to bogus log-in pages that are convincing replicas of legitimate websites.

"This was not a breach of internal Microsoft data," the Redmond, Washington-based technology firm said.

"Phishing is an industry-wide problem ... exercise extreme caution when opening unsolicited attachments and links from both known and unknown sources, and install and regularly update anti-virus software."

Microsoft is also advising Hotmail users to change their account passwords every 90 days.

Massive E-Mail Phishing Could Presage Bigger Attacks

In a situation that may still be developing, phishing exploits have hit Webmail services, including Gmail, Hotmail, Yahoo, AOL Mail, and others. As usual with mass phishing attacks - which aim to trick people into surrendering personal details about their online identities - it’s unclear what group or groups are behind the initiatives.

The one thing that is certain is the attacks are big.

"This is on a scale that is incredibly rare," said Mike Halsey, who runs The Long Climb, a PC support site in the U.K. "I don’t think it’s ever happened to this extent before, at least that I’m aware of."

The situation is unfolding rapidly. Halsey said a couple of days ago the site www.neowin.net reported that another site, www.pastebin.com, had posted personal details of about 20,000 users of Microsoft’s Hotmail, MSN and Windows Live services. Then on Tuesday, details about an additional 20,000 subscribers to Gmail, Yahoo, AOL Mail, Verizon and others were posted at the same site. The posts are now off-line.

It’s possible the criminals have details on many more users that they haven’t disclosed.

Details are sketchy, and there is no certainty that the problems are over. Sean-Paul Correll, a threat researcher with Panda Security, said he didn’t see any of the data from the attacks. But he noted that phishing attacks are often precursors to other initiatives.

"It is fairly common that this would be the first stage of a larger attack. They use these e-mail addresses for something else," he said. Correll added that identifying what group or groups are responsible depends upon seeing more of the infrastructure - such as the scripts they are using - than just e-mail addresses. He wasn’t sure what information might be available to researchers.

The next move is up to the criminals. Halsey pointed out that browser security is vital and the size of the apparently ongoing phishing attacks should serve as a warning to browser vendors, including Microsoft, Opera, Apple and Mozilla. Luckily, these companies are focusing on improving the security of their products.

While Halsey isn’t too worried about this week’s activities, he is concerned about the long-term impact. "I would say this is probably

isolated," he said of the phishing attacks. "The danger is that people pay a lot of attention when something like this is publicized but forget too quickly and do not learn. ... They shouldn't panic, or stop banking on the Internet or shopping on the Internet, as long as they are careful."

He added that good advice is available from a number of sources, including the British government, the FBI, and his site.

The key, according to Halsey, is to address the problem. "It is worrying from my point of view," he says. "It says people are not aware enough of what the threats are and that Internet service providers and major technology companies are not doing enough to warn people what the dangers are and how to avoid them, which is disappointing."

FBI Smashes US-Egypt Cyber 'Phishing' Ring

Investigators in the United States and Egypt have smashed a computer "phishing" identity theft scam described as the biggest cyber-crime investigation in US history, officials said Wednesday.

The Federal Bureau of Investigation said 33 people were arrested across the United States early Wednesday while authorities in Egypt charged 47 more people linked to the scam.

A total of 53 suspects were named in connection with the scam in a federal grand jury indictment, the FBI said.

Authorities said the sophisticated identity theft network had gathered information from thousands of victims which was used to defraud American banks.

Wednesday's arrests were the culmination of a two-year probe involving US and Egyptian officials dubbed "Operation Phish Phry."

The investigation was described in statement as the largest cybercrime investigation to date in the United States.

A series of raids early Wednesday resulted in arrests in California, Nevada and North Carolina.

A 51-count US indictment accuses all defendants with conspiracy to commit wire fraud and bank fraud while various defendants are charged with aggravated identity theft and conspiracy to commit computer fraud.

"The sophistication with which Phish Phry defendants operated represents an evolving and troubling paradigm in the way identity theft is now committed," FBI Los Angeles acting assistant director Keith Bolcar said.

"Criminally savvy groups recruit here and abroad to pool tactics and skills necessary to commit organized theft facilitated by the computer, including hacking, fraud and identity theft, with a common greed and shared willingness to victimize Americans."

According to an unsealed indictment, Egyptian-based hackers obtained bank account numbers and personal information from bank customers through phishing, and then hacked into accounts at two unidentified banks.

Once compromised accounts had been accessed, hackers in Egypt contacted conspirators based in the United States via text messages, phone calls and Internet chatrooms to arrange transfer of cash to fraudulent accounts.

"This international phishing ring had a significant impact on two banks and caused huge headaches for hundreds, perhaps thousands, of bank customers," acting US Attorney George Cardona said in a statement.

The investigation comes hard on the heels of a security breach targeting thousands of Microsoft Hotmail accounts.

Cyber-crooks evidently used "phishing" tactics to dupe users of Microsoft’s free Web-based email service into revealing account and access information, according to the US technology giant.

Threat of Next World War May Be in Cyberspace

The next world war could take place in cyberspace, the UN telecommunications agency chief warned Tuesday as experts called for action to stamp out cyber attacks.

"The next world war could happen in cyberspace and that would be a catastrophe. We have to make sure that all countries understand that in that war, there is no such thing as a superpower," Hamadoun Toure said.

"Loss of vital networks would quickly cripple any nation, and none is immune to cyberattack," added the secretary-general of the International Telecommunications Union during the ITU’s Telecom World 2009 fair in Geneva.

Toure said countries have become "critically dependent" on technology for commerce, finance, health care, emergency services and food distribution.

"The best way to win a war is to avoid it in the first place," he stressed.

As the Internet becomes more linked with daily lives, cyberattacks and crimes have also increased in frequency, experts said.

Such attacks include the use of "phishing" tools to get hold of passwords to commit fraud, or attempts by hackers to bring down secure networks.

Individual countries have started to respond by bolstering their defences.

US Secretary for Homeland Security Janet Napolitano said Thursday that she has received the green light to hire up to 1,000 cybersecurity experts to ramp up the United States’ defenses against cyber threats.

South Korea has also announced plans to train 3,000 "cyber sheriffs" by next year to protect businesses after a spate of attacks on state and private websites.

Warning of the magnitude of cybercrimes and attacks, Carlos Solari, Alcatel-Lucent’s vice-president on central quality, security and reliability, told a forum here that breaches in e-commerce are now already running to "hundreds of billions."

But one of the most prominent victims in recent years has been the small Baltic state of Estonia, which has staked some of its post Cold War development on new technology.

In 2007 a spate of cyber attacks forced the closure of government websites and disrupted leading businesses.

Estonian Minister for Economic Affairs and Communications Juhan Parts said in Geneva that "adequate international cooperation" was essential.

"Because if something happens on cyberspace... it’s a border crossing issue. We have to have horizontal cooperation globally," he added.

To this end, several countries have joined forces in the International Multilateral Partnership against Cyber Threats (IMPACT), set up this year to "proactively track and defend against cyberthreats."

Some 37 ITU member states have signed up, while another 15 nations are holding advanced discussions, said the ITU.

Experts say that a major problem is that the current software and web infrastructure has the same weaknesses as those produced two decades ago.

"The real problem is that we’re putting on the market software that is as vulnerable as it was 20 years ago," said Cristine Hoepers, general manager at Brazilian National Computer Emergency Response Team.

"If you see the vulnerabilities that are being exploited today, they are still the same," she underlined.

She suggested that professionals needed to be trained to "design something more resilient."

"Universities are not teaching students to think about that. We need to change the workforce, we need to go to the universities..., we need to start educating our professionals," she said.

Pointing out the infrastructure weakness, Carlos Moreira, who founded and runs the Swiss information security firm Wisekey, said legislation is needed to bring cybersecurity up to international standards.

Sony Claims New X Series Is the Lightest Laptop

There’s light, and then there’s light. Sony today rolled out its latest series of laptops VAIO X Series, which the company is touting as the world’s lightest. A separate line, the VAIO CW Series, is more suited for the average consumer.

The VAIO X Series is an ultraportable laptop that weighs in at 1.6 pounds and measures 7.29 inches by 10.95 inches by 0.55 inches with the standard battery. (A high-capacity battery option, when combined with the standard battery, will offer up to 15 hours of battery life, according to Sony.) The chassis is made of light-weight carbon fiber, with grooved edging along the sides, while the palmrest and the area around the keyboard is covered with an aluminum frame. Color options for the chassis include black and gold.

The touchpad offers multitouch functionality, allowing you to use finger gestures to zoom, rotate items, and scroll. The LED-backlit screen measures 11.1 inches (diagonal) and has a resolution of 1,366 by 768. The keyboard has a 17-mm key pitch.

The X Series features a 2-GHz Intel processor, 2 GB of DDR2 memory, an inte-grated Intel graphics chipset, and a 128-GB solid state drive. The system features a multimedia card reader, two USB 2.0 ports, and an Ethernet port, as well as a built-in webcam with face-tracking technology. Wireless capability includes 802.11b/g/n Wi-Fi and Bluetooth. The X Series lines also comes with 3G mobile broadband built in, though you'll have to get a separate Verizon Wireless subscrip-tion to use it. Interestingly enough, the X Series also comes with real-time GPS functionality.

On the more affordable side (at least for Sony) is the CW Series of laptops. The CW Series is aimed at the multimedia user on the go. The laptop measures 9.18 inches by 13.44 inches by between 1.09 to 1.52 inches, and weighs 5.3 pounds with the standard battery. It comes in five colors - red, pink, white, black, and indigo purple - and a glossy finish on the exterior.

The widescreen display measures 14.4 inches (diagonal), with a 16:9 aspect ratio. It also comes with a Blu-ray drive, as well as an HDMI port for hooking up to a big-screen HDTV. It has 3 USB ports, as well as outputs for VGA, FireWire (i.Link), and Ethernet. There is a multimedia card reader and a built-in Webcam, also with face-tracking technology.

The CW Series features a 2.2-GHz Intel Core 2 Duo T6600 processor, 4 GB of DDR3 memory (with a maximum of 8 GB available), a 500-GB, 5,400-RPM hard drive, and an Nvidia GeForce G210M discrete graphics card. The standard battery is estimated to last up to 4 hours, and the optional large-capacity battery is esti-mated to last up to 6 hours. The CW Series comes with both 802.11b/g/n and Bluetooth capability.

Both the X Series and CW Series will come equipped with Microsoft Windows 7 Home Premium (a 32-bit version for the X Series and the 64-bit option for the CW Series) and both are certified for EPEAT Gold and Energy Star 5.0. They are also RoHS-compliant.

The X Series will be available starting at $1,300 and can be pre-ordered on the Sony Style Web site. It will be available at Sony Style stores and select retailers in November. The CW Series starts at $780 and will be available in Sony Style stores and online, as well as at other retailers by the end of the month.

Microsoft Planning 128-Bit Version Of Windows 8?

Windows 7 is not even out the door yet and rumors are already circulating about the next version of Microsoft's OS, Windows 8.

According to Microsoft employee Robert Morgan, future iterations of Windows, including Windows 8, could support a 128-bit architecture. Two weeks ago his now defunct LinkedIn profile disclosed that he had been working on "research and development projects including 128-bit architecture compatibility with the Windows 8 kernel and Windows 9

project plan".

Further to this, Morgan’s profile also let slip that Microsoft are hoping to form a number of future relationships with major players such as IBM, Intel, AMD and others in the run up to 128-bit support. (Keep in mind that 64-bit computing is just now going mainstream.)

An interview with Robert Morgan, who has been with the company since 2002, is expected to appear on Windows 8 News within the coming days, hopefully shedding more light on what to expect from the next version of Windows, codenamed Chirdori.

Comcast Tries Pop-up Alerts To Warn of Infections

Comcast Corp. wants to enlist its customers in a fight against a huge problem for Internet providers - the armies of infected personal computers, known as "botnets," that suck up bandwidth by sending spam and facilitating cybercrime.

The country’s largest provider of high-speed Internet to homes started testing a service this week in Denver in which Comcast sends customers a pop-up message in their Web browsers if their computers seem to have been co-opted by a botnet. One botnet can have tens of thousands or even millions of PCs.

The message points to a Comcast site with tips for cleaning infected computers. It reads: "Comcast has detected that there may be a virus on your computer(s). For information on how to clean your computer(s), please visit the Comcast Anti-Virus Center."

Comcast said users can close the warning banners if they wish, but they cannot opt out of receiving them. A reminder will return every seven days while a computer appears to be infected.

The program, which Comcast hopes to roll out nationally, is one of the most aggressive moves yet by a major Internet provider to curb what’s become a scourge on the Internet.

Botnets are a part of most serious cybercrime. They’re used to steal credit card numbers, carry out so-called "denial-of-service" attacks that bring down Web sites and send spam by hijacking e-mail accounts and Internet connections.

A computer can fall into the sway of a botnet when it is infected with malicious software that puts the machine under the control of criminals, who use the anonymity provided by having so many zombie machines at their disposal to cover their tracks.

Comcast’s service is meant to block that step, by alerting customers to PC infections they likely didn’t know about because anti-virus software updates can’t keep up fast enough.

Comcast will try to detect a PC’s role in a botnet by studying how much data the machine is downloading and receiving.

"These cyber criminals have become so fast, a bot can be instructed to send out millions of spams in a matter of minutes," said Jay Opperman,

Comcast’s senior director of security and privacy. "The faster that we can detect these things are operating on our network, the better."

He said Comcast can tell the difference between a customer legitimately downloading a lot of video or other data and the malicious deeds of a bot-induced PC. One way is that the company checks the source of downloads, Opperman said, to compare them to a list of suspect sites that are known for spamming and other attacks. Opperman said Comcast will not look inside the content of the traffic, a controversial process called deep packet inspection.

Even so, the move could be risky, especially if Comcast’s program gets people to trust and respond to pop-up ads - which are often a vehicle for delivering the viruses that land an infected computer in a botnet. These phony ads often claim that a computer is infected and should be cleaned up with a click.

Comcast says its program contains an important secondary confirmation that the message is from the company and not a scammer: Comcast will send an e-mail to the customer’s primary e-mail account.

However, Phil Lin, marketing director at network security firm FireEye Inc., said hackers could mimic Comcast’s pop-up banner or the confirmation ads. And unsuspecting customers wouldn’t know they should expect to see a confirmation from Comcast in the first place.

No Facebook at Work in Most US Companies

More than half of US companies do not allow employees to visit social networks such as Facebook, MySpace or Twitter while at work, according to a new survey.

Fifty-four percent of the chief information officers (CIOs) for 1,400 companies surveyed across the United States said workers were "prohibited completely" from visiting social networks while on the job.

Nineteen percent said employees were allowed to visit social networks "for business purposes only" while 16 percent said they allowed "limited personal use."

Ten percent of those surveyed said there were no restrictions on visiting social networks at work.

The survey of 1,400 companies with at least 100 employees was released this week and was conducted by an independent research firm for Robert Half Technology, a California-based provider of information technology professionals. It has a margin of error of plus or minus 2.6 percent.

Dave Willmer, executive director of Robert Half Technology, said "using social networking sites may divert employees’ attention away from more pressing priorities, so it’s understandable that some companies limit access.

"For some professions, however, these sites can be leveraged as effective business tools, which may be why about one in five companies allows their use for work-related purposes," he said.

Reminder: Create Strong Passwords! Here's How

The recent password compromises of Hotmail, GMail and (from other reports I've read) Yahoo! Mail make this a good time to revisit the issue of passwords.

The webmail services in these cases are saying that phishing is the likely cause of the breach. Security firm ScanSafe thinks that there are other possibilities, but I think it's reasonable to believe phishing is the culprit here, and certainly phishing is a major problem, as evidenced by yesterday's arrests in the US and Egypt.

Passwords are collected by the bad guys in many ways, such as by malware that scans the system and monitors Internet usage for usernames and passwords. Dictionary attacks are also used to guess passwords from a list of common ones. But in this case only webmail credentials were found. Webmail systems are tough to attack with dictionary attacks because they won't let you attempt login after login trying different credentials.

If your password is collected by phishing or through malware finding it on your computer or snooping it as you type it on a form, a strong password does you no good. Whether the password is strong or weak you have to make an effort to protect it on your system and not to give it away to the wrong people. Apart from some security savvy for recognizing threats, for most people the best defense is to use a good security suite and to keep it updated. These will make it much harder for malware to get on your system or to run unimpeded if it does. Most of them also detect and block phishing attempts.

But you still want to have strong passwords. There are places where weak passwords can be compromised, such as the login for your PC. Now very few people, including the experts, do all the things experts tell them to do in this regard. After all, it's inconvenient.

Acunetix analyzed the leaked list of Hotmail passwords and found that lots of the users use weak passwords. The most popular password in the list (64 of them) was '123456' which, after 'password', is the all-time classic weak password. Interestingly there were 11 instances of 'alejandra' and lots of Spanish words and names, perhaps saying something about the phishing campaign used to obtain the accounts.

How do you choose a strong password? Here are some guidelines:

* The longer the better: At least 8 characters.

* Mix upper and lower case, punctuation and numerals.

* One good way to implement both of the first two rules is with a /passphrase/, i.e. a sentence instead of a word: "I hate passw0rds, they suck" or "My father was born in 1929." I use these in a few places but, alas, not all sites allow you that long a password or to embed spaces.

* Avoid passwords that are words in a dictionary, especially common words.

* Avoid reusing passwords, especially those for critical resources like your e-mail, on other sites. Doing this exposes you to a wider compromise than necessary.

Most of us don't have the memory bandwidth to deal with a large number of obscure passwords, so a good next step is to use a password management program, such as Roboform or the open source Password Safe. Some suites, like Norton Internet Security 2010, include password management in them. These programs let you auto-generate strong passwords and it remembers them for you; you just remember a master password.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.